lultiple input shift register for check-sum calculation

Publication number: DE19722157 (A1)
Publication date: 1998-12-10
Inventor(s): KNUTH ROBERT [DE] +
Applicant(s): SIEMENS AG [DE] +
Classification:
- international: ***G11C19/00;*** **G11C19/00;** (IPC1-7): G11C19/28
- European: G11C19/00
Application number: DE19971022157 19970527
Priority number(s): DE19971022157 19970527

Abstract of **DE 19722157 (A1)**

The shift register (M2) forms a check-sum (Z (t)) in dependence on n times m simultaneously supplied digital input signals (x1 (t). , xnm (t)), a number of m shift registers (R1. ,Rm) are clocked with a first period t, and their contents (z1 (t). , zm (t)) form the check-sum. A number of n of the input signals are respectively supplied to the shift register between each pair of the m registers. The architecture of the shift register is determined through a certain equation system, which is based on a recursive calculation of the check-sum.

---

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 197 22 157 A 1**

(51) Int. Cl.[6]: **G 11 C 19/28**

(21) Aktenzeichen: 197 22 157.2
(22) Anmeldetag: 27. 5. 97
(43) Offenlegungstag: 10. 12. 98

DE 197 22 157 A 1

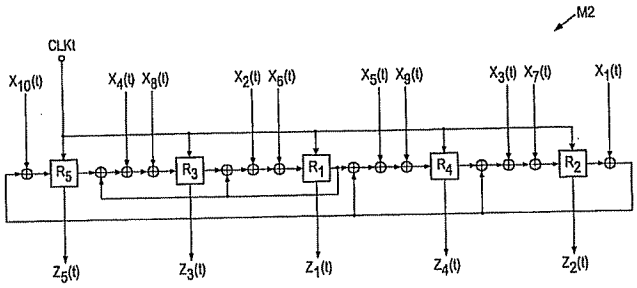
(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Knuth, Robert, 81737 München, DE

(56) Entgegenhaltungen:
US-Z.: IBM Journal of Research and Development, Vol. 34 No. 2/3, March/May 1990, S. 363-380;

(54) Multiple Input Shift Register zur Bildung einer Prüfsumme

(57) Multiple Input Shift Register M2 zur Bildung einer Prüfsumme Z(t) in Abhängigkeit von n x m gleichzeitig zugeführten digitalen Eingangssignalen $x_1(t)$, ..., $x_{nm}(t)$ mit m > 1 mit einer Periode t getakteten Schieberegistern R1, ..., Rn, deren Inhalte $z_1(t)$, ..., $z_m(t)$ in der Periode t die Prüfsumme $Z(t) = (z_1(t), ..., z_m(t))$ bilden. Ihm werden zwischen je zweien der m Register jeweils $n = 2^a$, $a \geq 1$, der Eingangssignale $x_1(t)$, ..., $x_{nm}(t)$ zugeführt. Seine Architektur ist bestimmt durch ein Gleichungssystem, das durch a-faches rekursives Einsetzen von Z(t-i), i = 1, 2, ..., a, in das Gleichungssystem $Z(t) = C \cdot Z(t-1) \oplus X(t-1)$ eines herkömmlichen MISRs M2 mit einem Eingang je Register gebildet ist. Dabei weist jeder Vektor $X(t-2)=(x_k(t-2), ..., x_{k+m}(t-2))$, k=2, ..., n, jeweils m andere der n x m Eingangssignale $x_2(t)$, ..., $x_{nm}(t)$ auf. Nach Durchführung der a Rekursionen wird Z(t-a) durch Z(t-2) ersetzt. Vorteil: Die Prüfsumme und die Wahrscheinlichkeit, daß sie auch bei fehlerhaften Eingangssignalen korrekt ist, ist dieselbe, wie beim herkömmlichen MISR M2.



DE 197 22 157 A 1

Beschreibung

Die Erfindung betrifft ein Multiple Input Shift Register (MISR), auch Multiple Input Signature Register genannt, zur Bildung einer Prüfsumme.

Fig. 1 zeigt ein herkömmliches MISR M1 vom Grad m = 5. Es weist m = 5 Register R1,. . .,R5 auf, die ein mit einer Periode T eines Taktes CLKT getaktetes Schieberegister bilden, wobei zusätzliche Rückkopplungszweige vorhanden sind. Zwischen je zweien der Register R1,. . .,R5 ist eine XOR-Verknüpfung (Exclusive OR, Exklusives ODER) mit jeweils einem Eingang angeordnet, an den je eines der fünf digitalen Eingangssignale $x_1(T)$,. . .,x_5 (T) des MISR anlegbar ist. Zu jeder Periode T bilden die Inhalte der Register eine Prüfsumme Z (T) = (z_1 (T),. . .,z_5 (T)).

Die Architektur eines beliebigen MISR vom Grad m kann durch folgende Gleichung beschrieben werden (vgl. Daehn et al. Aliasing errors in linear automata used as multiple-input signature analyzers, in: IBM, Journal of Research and Development, Vol. 34, Nr. 2/3, März/Mai 1990, S. 363ff.):

$$Z(T) = C \cdot Z(T-1) \oplus X(T-1).$$

Dabei ist C eine quadratische Koeffizientenmatrix mit der Kantenlänge m (sogenannte "next-state matrix"). Für das Beispiel des herkömmlichen MISR in **Fig.** 1 lautet diese Gleichung

$$(1) \qquad Z(T) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} z_1(T-1) \\ z_2(T-1) \\ z_3(T-1) \\ z_4(T-1) \\ z_5(T-1) \end{bmatrix} \oplus \begin{bmatrix} x_1(T-1) \\ x_2(T-1) \\ x_3(T-1) \\ x_4(T-1) \\ x_5(T-1) \end{bmatrix}.$$

Um on-chip eine Überprüfung der Funktionsfähigkeit von integrierten Schaltungen vornehmen zu können, werden diese mit einem MISR versehen. Digitale Ausgangssignale der zu überprüfenden Schaltung werden dem MISR in jeder Periode T als dessen Eingangssignale zugeführt. Nach k Perioden T beträgt bei einem herkömmlichen MISR vom Grad m mit je einem Eingang je Register die Wahrscheinlichkeit P_{alias}, daß falsche Eingangssignale zu derselben Prüfsumme Z(T) führen wie korrekte Eingangssignale

$$P_{alias} = (2^{k-m}-1)/(2^k-1),$$

wie einfach herzuleiten ist. In der Praxis wählt man $k \gg m$, so daß näherungsweise gilt

$$P_{alias} = 2^{-m}.$$

Für eine ausreichend geringe Wahrscheinlichkeit P_{alias} für das Nichterkennen von auftretenden Fehlern von 1 ppm muß das herkömmliche MISR folglich mindestens eine Länge von m = 20 Registern aufweisen. Da bei MISRs mit je einem Eingang je Register (im folgenden "herkömmliche MISRs" genannt) bei mehr als 20 Eingangssignalen weitere Register benötigt werden, wird in diesen Fällen eine unnötig geringe Wahrscheinlichkeit P_{alias} erzielt. Gleichzeitig nimmt der Flächenbedarf des MISR aufgrund der zusätzlichen Register zu.

Um eine größere Anzahl von Eingangssignalen bei einem MISR mit vorgegebener Registeranzahl zu ermöglichen, ist es möglich, XOR-Verknüpfungen mit mehr als einem Eingang zwischen je zweien der Register vorzusehen. Für diese läßt sich eine Wahrscheinlichkeit für das Auftreten identischer Prüfsummen bei voneinander abweichenden Eingangssignalen jedoch nur sehr aufwendig bestimmen.

Der Erfindung liegt daher die Aufgabe zugrunde, ein MISR anzugeben, welches eine größere Anzahl von Eingängen als Register aufweist und bei dem die Wahrscheinlichkeit für das Auftreten "korrekter" Prüfsummen bei falschen Eingangssignalen in einfacher Weise bestimmbar ist.

Die Aufgabe wird durch ein MISR gemäß Anspruch 1 gelöst. Weiterbildungen und Ausgestaltungen der Erfindung sind in den Unteransprüchen gekennzeichnet.

Demnach ist ein MISR zur Bildung einer Prüfsumme Z(t) in Abhängigkeit von n × m gleichzeitig an entsprechende Eingänge anlegbaren digitalen Eingangssignalen x_1 (t),. . .,x_{nm}(t) vorgesehen,

- mit m > 1 mit einer Periode t getakteten Schieberegistern, deren Inhalte z_1(t),. . .,z_m(t) in der Periode t die Prüfsumme Z(t)=(z_1(t),. . .,z_m(t)) bilden,
- bei dem zwischen je zweien der m Register jeweils $n = 2^a$, $a \geq 1$ der Eingänge des MISR angeordnet sind,
- dessen Architektur bestimmt ist durch ein Gleichungssystem, das durch a-faches rekursives Einsetzen von Z(t–i), i=1, 2,. . .,a, in das Gleichungssystem

$$Z(t) = C \cdot Z(t-1) \oplus X(t-1)$$

gebildet ist,

- wobei jeder Vektor X(t–i) = (x_k(t–1),. . .,x_{k+m}(t–1)), k=1,. . .,n, an jeweils m anderen der n × m Eingänge anlegbare der Eingangssignale x_1(t),. . .,x_{nm}(t) aufweist,
- wobei nach Durchführung der a Rekursionen Z(t–a) durch Z(t–1) ersetzt wird,

– wobei

$$Z(T) = C \cdot Z(T-1) \oplus X(T-1)$$

die Architektur eines herkömmlichen MISR beschreibt mit m mit einer Periode T getakteten Schieberegistern,
– bei dem zwischen jeweils zweien der Register höchstens ein Eingang angeordnet ist, so daß gleichzeitig höchstens m Eingangssignale $X(T)=(x_1(T),\ldots,x_m(T))$ an das MISR anlegbar sind,
– bei dem die Inhalte $z_1(T),\ldots,z_m(T)$ der Register zum Zeitpunkt T eine Prüfsumme $Z(T)=(z_1(T),\ldots,z_m(T))$ bilden,
und für das C eine Koeffizientenmatrix der Dimension $m \times m$ ist.

Die Erfindung bietet den Vorteil, daß beim erfindungsgemäßen MISR für die Korrektheit der Prüfsumme Z(T) auch bei fehlerhaften Eingangssignalen dieselbe Wahrscheinlichkeit P_{alias} gilt, wie bei einem herkömmlichen MISR mit nur einem Eingang je Register, dessen Next-State Matrix C zur Ermittlung der das erfindungsgemäße MISR beschreibenden Gleichung verwendet wird. Der Beweis hierfür wird weiter unten anhand des Ausführungsbeispiels in **Fig.** 2 geführt.

Somit ermöglicht die Erfindung die Konstruktion eines MISR mit mehr als einem Eingang je Register, für welches ohne Schwierigkeit die Wahrscheinlichkeit P_{alias} angegeben werden kann. Dies liegt daran, daß, wie bereits erwähnt, für herkömmliche MISR die Wahrscheinlichkeit P_{alias} in einfacher Weise bestimmbar ist.

Nach einer Weiterbildung der Erfindung ist es vorgesehen, daß bei dem MISR je zwei der Register über eine XOR-Verknüpfung miteinander verbunden sind, die höchstens n Eingänge aufweist, die die Eingänge des MISR sind.

Nach einer anderen Ausgestaltung der Erfindung ist bei dem MISR für diejenigen Eingangssignale x(t), die in jeder Periode t einen niedrigen oder in jeder Periode t einen hohen Pegel haben, kein Eingang der entsprechenden XOR-Verknüpfung vorgesehen. Es sind dann weniger als n Eingänge je Register des MISR für die $n \times m$ Eingangssignale vorhanden.

Die Erfindung wird im folgenden anhand eines Ausführungsbeispiels näher erläutert. Es zeigen:

Fig. 1 ein herkömmliches MISR nach dem oben beschriebenen Stand der Technik,

Fig. 2 ein erstes Ausführungsbeispiel eines erfindungsgemäßen MISRs,

Fig. 3 eine Abwandlung des MISR aus **Fig.** 1 mit einem Multiplexer und

Fig. 4 ein zweites Ausführungsbeispiel gemäß der Erfindung.

Fig. 2 zeigt ein erfindungsgemäßes MISR M2 vom Grad m = 5, welches m = 5 mit einer Periode t eines Taktes CLKt getaktete Schieberegister R1,...,R5 aufweist, deren Inhalte $z_1(t),\ldots,z_5(t)$ in der Periode t eine Prüfsumme $Z(t) = (z_1(t),\ldots,z_5(t))$ bilden. Das MISR M2 weist zehn Eingänge zum Anlegen zehn entsprechender digitaler Eingangssignale $x_1(t),\ldots,x_{10}(t)$ auf.

Die Architektur des MISR M2 in **Fig.** 2 ist bestimmt durch ein Gleichungssystem, das durch einmaliges rekursives Einsetzen von Z(T–1) in das Gleichungssystem

$$Z(T) = C \cdot Z(T-1) \oplus X(T-1) \quad (1)$$

des herkömmlichen MISR Ml aus **Fig.** 1 gebildet ist, bei dem zwischen jeweils zweien der Register R1,...,R5 ein Eingang angeordnet ist. Es ergibt sich als Ergebnis der Rekursion:

$$Z(T) = C \cdot (C \cdot Z(T-2) \oplus X(T-2)) \oplus X(T-1).$$

Durch Einsetzen von

$$X(T-2) = Y(t-1) = (x_1(t-1),\ldots,x_5(t-1))$$
$$X(T-1) = X(t-1) = (x_6(t-1),\ldots,x_{10}(t-1))$$
$$Z(T) = Z(t) \text{ und}$$
$$Z(T-2) = Z(t-1)$$

ergibt sich daraus

$$Z(t) = C \cdot (C \cdot Z(t-1) \oplus Y(t-1)) \oplus X(t-1) \quad (2)$$
$$\Rightarrow Z(t) = (C \cdot C \cdot Z(t-1)) \oplus (C \cdot Y(t-1)) \oplus X(t-1).$$

Bei diesem Ausführungsbeispiel wird vom herkömmlichen MISR M1 aus **Fig.** 1 ausgegangen. Mit der zugehörigen Next-State Matrix C (s. Gleichung (1)) ergibt sich hieraus für das erfindungsgemäße MISR M2 in **Fig.** 2

$$Z(t) = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} z_1(t-1) \\ z_2(t-1) \\ z_3(t-1) \\ z_4(t-1) \\ z_5(t-1) \end{bmatrix} \oplus \begin{bmatrix} x_2(t-1) \\ x_1(t-1) \oplus x_3(t-1) \\ x_4(t-1) \\ x_1(t-1) \oplus x_5(t-1) \\ x_1(t-1) \end{bmatrix} \oplus \begin{bmatrix} x_6(t-1) \\ x_7(t-1) \\ x_8(t-1) \\ x_9(t-1) \\ x_{10}(t-1) \end{bmatrix}.$$

Diese Gleichung gibt die Architektur des MISR M2 aus **Fig.** 2 an. Man erhält sie mit nur wenigen Umformungsschrit-

ten, wobei von der Next-State Matrix C eines herkömmlichen MISR M1 Gebrauch gemacht wird.

Die Erfindung bietet den Vorteil, daß für die Prüfsumme Z(T) des erfindungsgemäßen MISR M2 dieselbe Wahrscheinlichkeit P_{alias} gilt, wie für das herkömmliche MISR M1, dessen Next-State Matrix C verwendet wird. Dies liegt daran, daß sich in beiden Fällen auch dieselbe Prüfsumme ergibt, wenn beim erfindungsgemäßen MISR während jeder Periode t jeweils gleichzeitig die Eingangssignale angelegt werden, die dem herkömmlichen MISR M1 in jeweils zwei aufeinander folgenden Perioden zugeführt werden.

Zum Beweis hierfür wird **Fig.** 3 betrachtet, die das herkömmliche MISR M1 aus **Fig.** 1 mit einem seinen Eingängen vorgeschalteten Multiplexer MUX zeigt. Mittels des Multiplexers halb so schnell wie das MISR M1 getakteten Multiplexer MUX ist es möglich, in zwei aufeinander folgenden Perioden T nacheinander je n = S verschiedene Eingangssignale $x_1(T),\ldots,x_5(T)$; $x_6(T),\ldots,x_{10}(T)$ dem MISR M1 zuzuführen. Für die Schaltung aus **Fig.** 3 gilt also für zwei aufeinander folgende Taktperioden T, T+1:

$$Z(T+1) = C \cdot (C \cdot Z(T-1) \oplus X(T-1)) \oplus X(T)$$
$$\Rightarrow Z(T+1) = ((C \cdot C) \cdot Z(T-1) \oplus (C \cdot X(T-1))) \oplus X(T)$$

$$\Rightarrow Z(T+1) = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} z_1(T-1) \\ z_2(T-1) \\ z_3(T-1) \\ z_4(T-1) \\ z_5(T-1) \end{bmatrix} \oplus \begin{bmatrix} x_2(T-1) \\ x_1(T-1) \oplus x_3(T-1) \\ x_4(T-1) \\ x_1(T-1) \oplus x_5(T-1) \\ x_1(T-1) \end{bmatrix} \oplus \begin{bmatrix} x_1(T) \\ x_2(T) \\ x_3(T) \\ x_4(T) \\ x_5(T) \end{bmatrix}.$$

Die Prüfsumme Z(T) wird für die Schaltung in **Fig.** 3 also durch Rekursion auf dieselbe Art gebildet, wie die Prüfsumme Z(t) beim erfindungsgemäßen MISR M2 aus **Fig.** 2, ohne daß die oben genannten Substitutionen durchgeführt werden. Es liegt auf der Hand, daß hierbei die Wahrscheinlichkeit P_{alias} nicht beeinflußt wird, so daß sie in beiden Fällen übereinstimmt. Bei der Erfindung ist aufgrund der bei der Durchführung der Rekursion durchgeführten Substitutionen kein Multiplexer notwendig und es ist möglich, eine doppelt so große Anzahl von Eingangssignalen während derselben Taktperiode t dem erfindungsgemäßen MISR M2 zuzuführen wie dem herkömmlichen MISR M1.

Das erfindungsgemäße MISR M2 kommt somit entweder mit halb so vielen Registern R1,...,Rm aus wie das herkömmliche MISR M1 oder kann bei gleicher Registeranzahl halb so schnell getaktet werden, um dieselbe Anzahl von Eingangssignalen zu verarbeiten.

Fig. 4 zeigt ein zweites Ausführungsbeispiel der Erfindung, das sich von demjenigen in **Fig.** 2 nur insofern unterscheidet, als zweien der Register R1,...,R5 weniger als n = 2 Eingänge zugeordnet sind. Die entsprechenden Eingangssignale weisen für alle Perioden T einen hohen bzw. niedrigen Pegel auf. Im vorliegenden Fall gilt für alle Perioden t (vgl. **Fig.** 2): $x_9(t)=1$, $x_{10}(t)=0$.

Es wird betont, daß bei diesem Ausführungsbeispiel zwar vom herkömmlichen MISR M1 in **Fig.** 1 ausgegangen wird. Es ist aber selbstverständlich möglich, die Next-State Matrix C anderer herkömmlicher MISR zu verwenden. Es ist dabei möglich, die Registeranzahl frei zu wählen und auch die Art der Rückkopplungen. Beides beeinflußt nur die Next-State Matrix C.

Weiterhin ist es möglich, in die Gleichung (2) wenigstens ein weiteres Mal auf analoge Weise rekursiv einzusetzen. Man erhält dann die Gleichung für ein MISR mit jeweils vier Eingangssignalen je Register. Mit jeder Rekursion erfolgt eine Verdopplung der Anzahl der Eingänge je Register.

Patentansprüche

1. Multiple Input Shift Register (M2) zur Bildung einer Prüfsumme Z(t) in Abhängigkeit von n × m gleichzeitig zugeführten digitalen Eingangssignalen $x_1(t),\ldots,x_{nm}(t)$,
   - mit m > 1 Schieberegistern $(R_1,\ldots,R_m)$, die mit einer Periode t getaktet sind und deren Inhalte $z_1(t),\ldots,z_m(t)$ in der Periode t die Prüfsumme $Z(t)=(z_1(t),\ldots,z_m(t))$ bilden,
   - dem zwischen je zweien der m Register $(R_1,\ldots,R_m)$ jeweils $n = 2^a$, $a \geq 1$, der Eingangssignale $x_1(t),\ldots,x_{nm}(t)$ zugeführt werden,
   - dessen Architektur bestimmt ist durch ein Gleichungssystem, das durch a-faches rekursives Einsetzen der Prüfsummen Z(t–i), i=1, 2,...,a, in das Gleichungssystem

     $$Z(t) = C \cdot Z(t-1) \oplus X(t-1)$$

     gebildet ist,
   - wobei nach Durchführung der a Rekursionen
     - jedes X(t–i) durch $X(t-1) = (x_k(t-1),\ldots,x_1(t-1))$ mit jeweils m anderen der n × m Eingangssignale $x_1(t),\ldots,x_{nm}(t)$ ersetzt wird
     - und Z(t–a) durch Z(t–1) ersetzt wird,
   - wobei

     $$Z(T) = C \cdot Z(T-1) \oplus X(T-1)$$

die Architektur eines Multiple Input Shift Registers (M1) beschreibt mit m mit einer Periode T getakteten Schieberegistern,

- bei dem zwischen jeweils zweien der Register höchstens ein Eingangssignal zugeführt wird, so daß ihm gleichzeitig höchstens m Eingangssignale $X(T)=(x_1(T),\ldots,x_m(T))$ zugeführt werden,
- bei dem die Inhalte $z_1(T),\ldots,z_m(T)$ der Register zum Zeitpunkt T eine Prüfsumme $Z(T)=(z_1(T),\ldots,z_m(T))$ bilden,

- und für das C eine Koeffizientenmatrix der Dimension $m \times m$ ist.

2. Multiple Input Shift Register nach Anspruch 1, bei dem je zwei der Register über eine XOR-Verknüpfung miteinander verbunden sind, wobei die Eingangssignale $x_1(t),\ldots,x_{nm}(t)$ Eingängen der XOR-Verknüpfungen zugeführt werden.

3. Multiple Input Shift Register nach Anspruch 2, bei dem für diejenigen Eingangssignale x(t), die in jeder Periode t einen niedrigen oder in jeder Periode t einen hohen Pegel haben, kein Eingang der entsprechenden XOR-Verknüpfung vorgesehen ist.

4. Multiple Input Shift Register nach einem der vorstehenden Ansprüche,

- bei dem die Anzahl der Rekursionen a = 1 beträgt, so daß die Anzahl der Eingangssignale zwischen je zweien der Register $(R_1,\ldots,R_m)$ n = 2 ist,
- und dessen Architektur bestimmt ist durch

$$Z(t) = C \cdot (C \cdot Z(t-1) \oplus Y(t-1)) \oplus X(t-1),$$

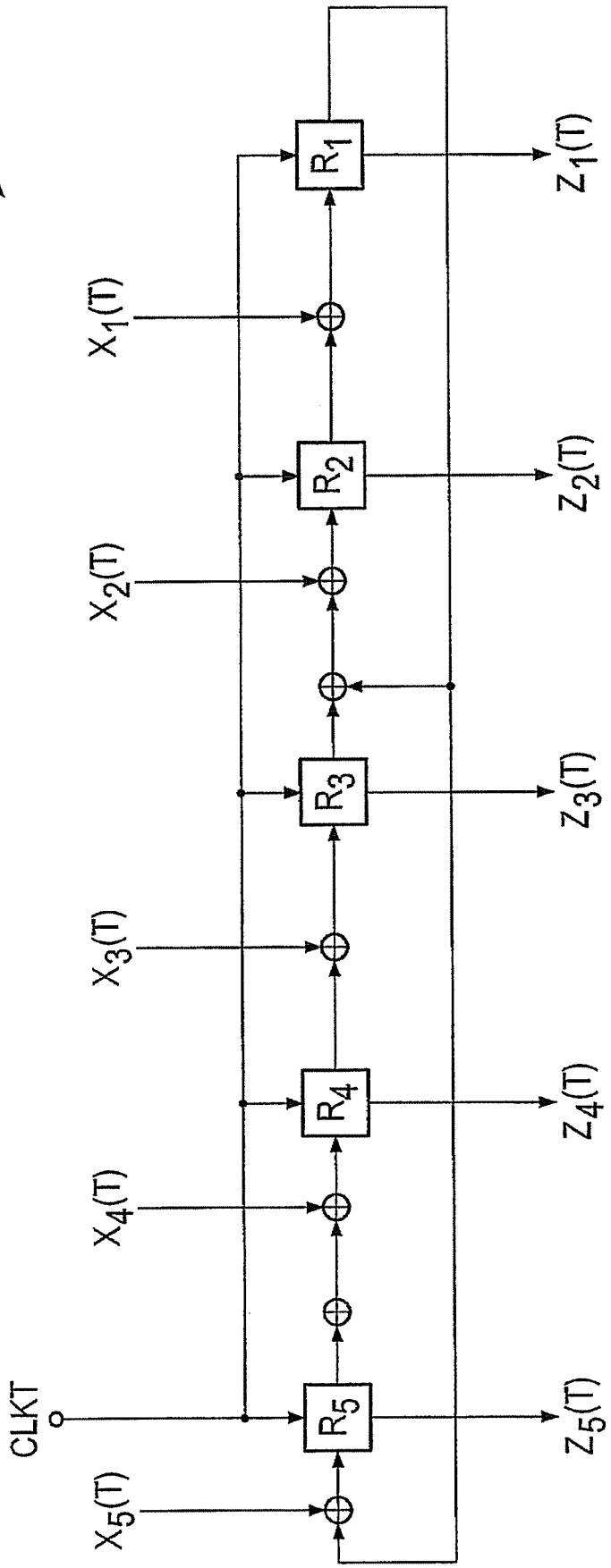
- wobei Y(t), X(t) Vektoren sind, die jeweils m der zum Zeitpunkt t an die Eingänge anlegbaren 2m Eingangssignale enthalten.

Hierzu 4 Seite(n) Zeichnungen

- Leerseite -

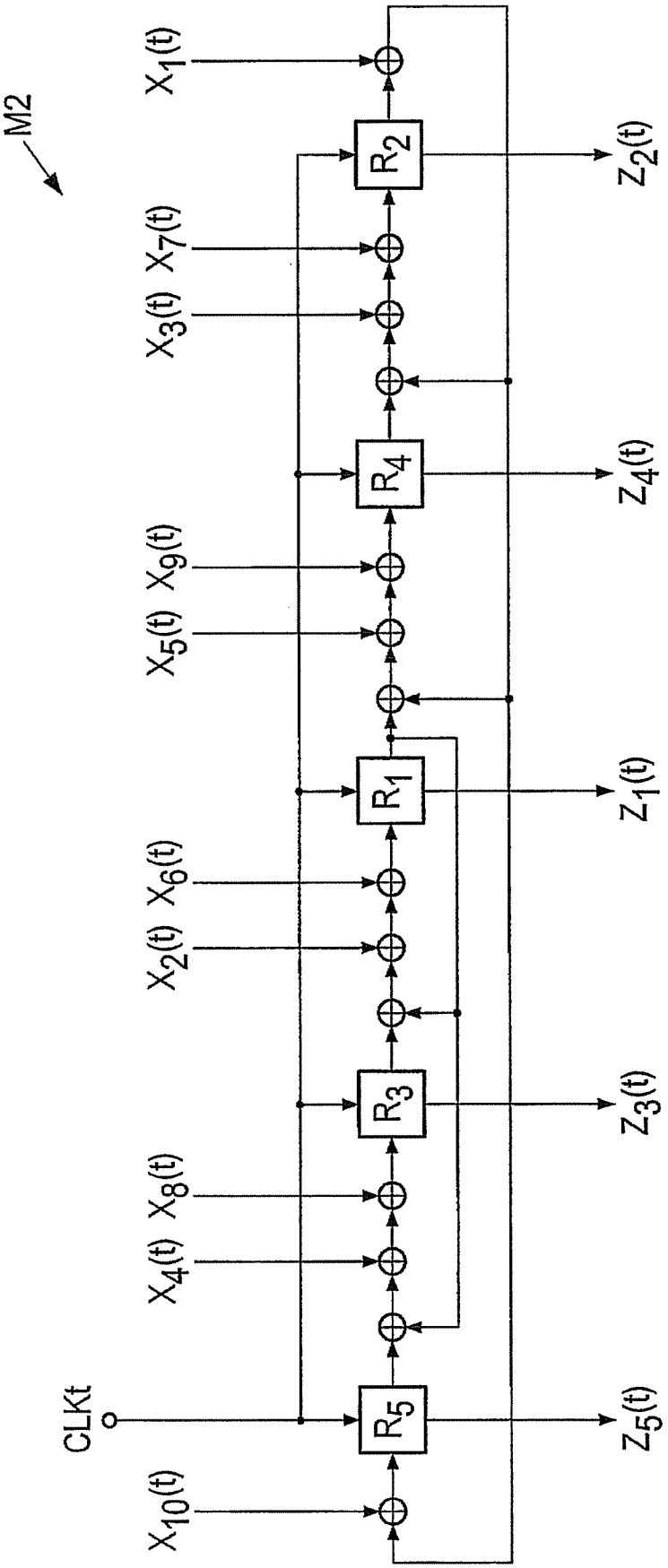
Nummer: DE 197 22 157 A1
Int. Cl.[6]: G 11 C 19/28
Offenlegungstag: 10. Dezember 1998

FIG 1



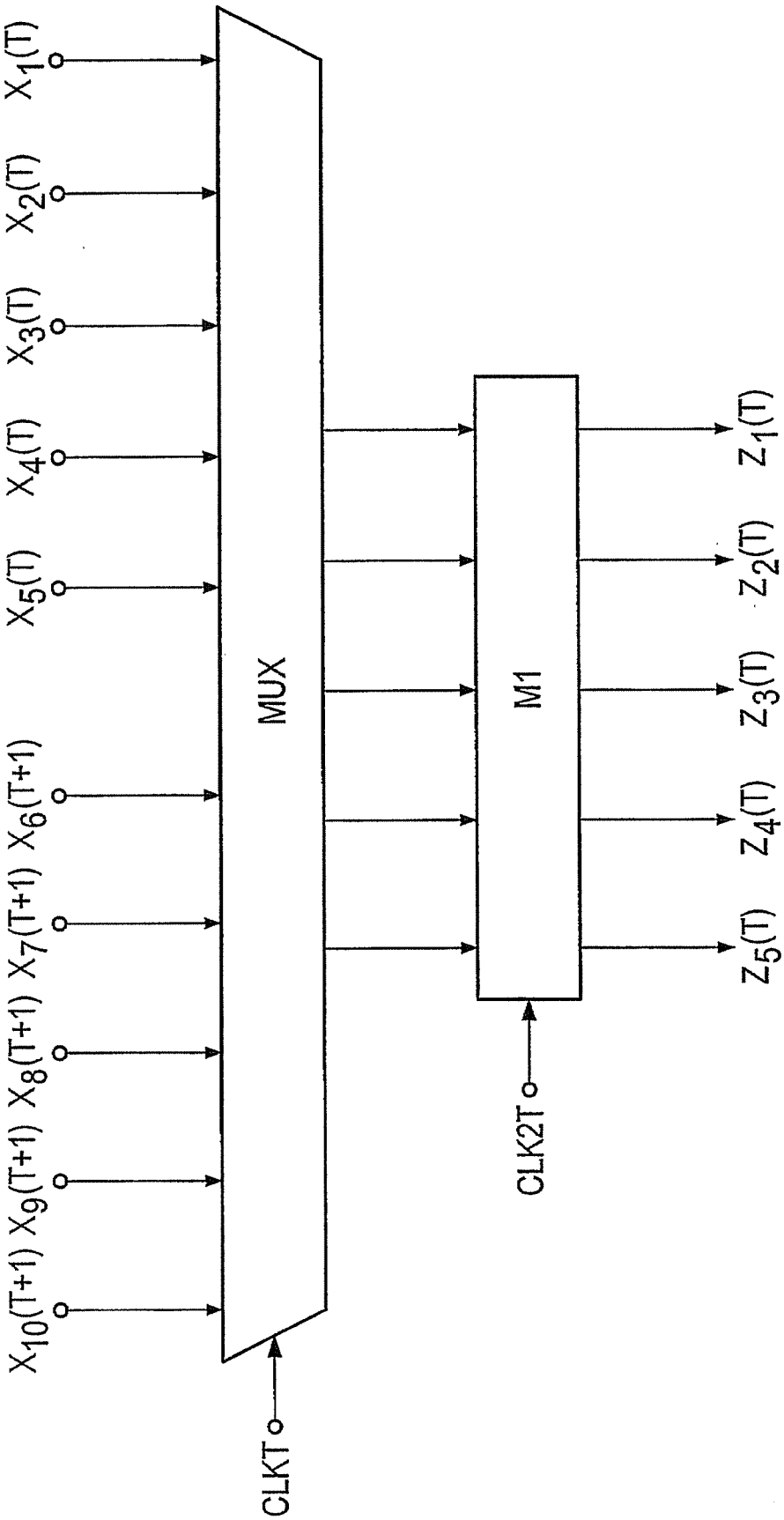
Nummer: DE 197 22 157 A1
Int. Cl.[6]: G 11 C 19/28
Offenlegungstag: 10. Dezember 1998

FIG 2



Nummer: DE 197 22 157 A1
Int. Cl.[6]: G 11 C 19/28
Offenlegungstag: 10. Dezember 1998

FIG 3



Nummer: DE 197 22 157 A1
Int. Cl.[6]: G 11 C 19/28
Offenlegungstag: 10. Dezember 1998

FIG 4